B6

(12) UK Patent Application (19) GB (11) 2 326 011 (13) A

(43) Date of A Publication 09.12.1998

(21) Application No 9811597.5

(22) Date of Filing 01.06.1998

(30) Priority Data
(31) 19723862 (32) 06.06.1997 (33) DE

(51) INT CL[6]
G07F 7/10

(52) UK CL (Edition P)
G4V VAK
G4H HTG H1A H13D H14A H14B H14D

(56) Documents Cited
US 5578808 A US 5036461 A US 4969188 A

(58) Field of Search
UK CL (Edition P) G4V VAK
INT CL[6] G07F 7/10
ONLINE:WPI

(71) Applicant(s)
International Business Machines Corporation
(Incorporated in USA - New York)
Armonk, New York 10504, United States of America

(72) Inventor(s)
Hermann Bublitz
Steven G Lee
Adam R Newth

(74) Agent and/or Address for Service
P Waldner
IBM United Kingdom Limited, Intellectual Property Department, Hursley Park, WINCHESTER, Hampshire, SO21 2JN, United Kingdom

(54) Abstract Title
Mobile data carrier for security modules

(57) A mobile data carrier (6), such as a chip card, with a processor, a memory and an interface, is capable of insertion in a terminal (1), and capable of exchanging data with the terminal (1) via the interface. At least two security modules (7,8) are disposed on the mobile data carrier (6) each comprising security-related data and/or security-related functions. With the at least two security modules (7,8) applications which comprise the use of a terminal (1) are performable. The terminal operating system may determine which module is to be used for a particular application and each module may be protected by a password. Where the terminal is used for electronic value exchange a function may be included to provide a credit limit.

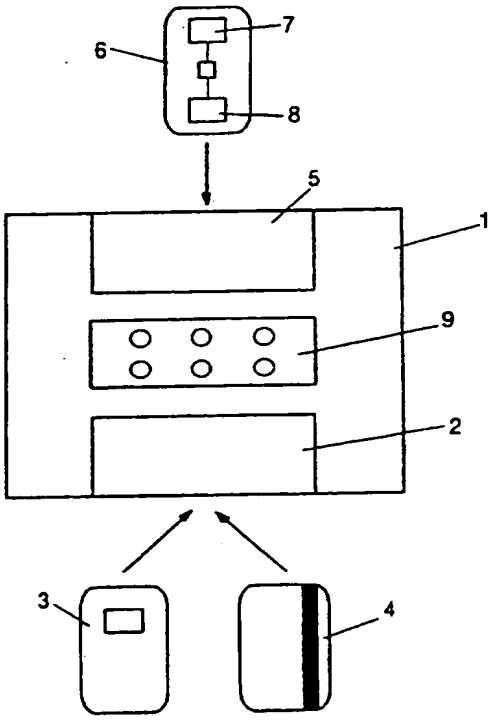

FIG. 1

GB 2 326 011 A

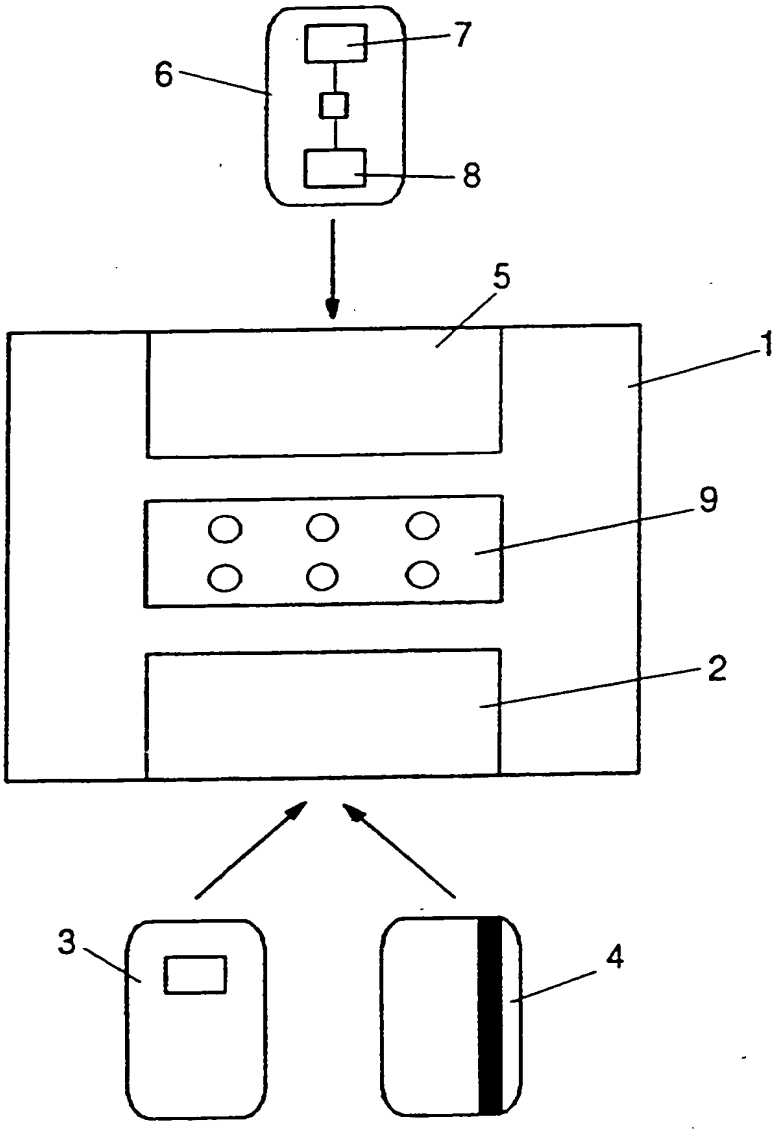

FIG. 1

2326011

MOBILE DATA CARRIER FOR SECURITY MODULES

This invention concerns a mobile data carrier, particularly a chip card, with a processor, a memory and an interface. The mobile data carrier is capable of insertion in a terminal and of exchanging data with the terminal via the interface.

Such mobile data carriers are used, for example, in combination with an electronic exchange. The electronic exchange is a modern method of cashless payment for goods and services, wherein a financial institution which owns the electronic exchange issues a chip card to a customer and registers the customer's data on the issued chip card. The data to be registered includes, in particular, the manner of use of the chip card, the credit limit, the period of validity and the accounting method.

Prior to its issue to the customer, the chip card is initialized, i.e. application data is entered on the chip card which enables the chip card to be used within the limits of particular applications. Upon the issue of the chip card, the customer is informed of the applications for which the chip card can be used.

In order that the chip card can be used for paying for goods and services, some money must first be stored on the chip card. For this purpose, the customer transfers a determinate amount of money as cash at a service facility of the financial institution, or has that determinate amount debited from his account. A credit balance equal to the determinate amount is then stored on the chip card. The customer can then use the chip card for payment up to that amount. The financial institution remits the same determinate amount to an exchange account. A merchant subsequently receives his money from this exchange account when the customer has paid this merchant using the chip card.

Once the credit is used up, the chip card must be "recharged".A credit can be entered on to the chip card by a service facility clerk of the financial institution, by means of an appropriate input terminal. Any automatic bank tellers equipped with this function can also be used for this purpose.

If, subsequently, the customer wishes to pay for goods using his chip card in a merchant's shop, this transaction can be executed at a POS

terminal (point-of-sale terminal). The chip card is inserted into a chip card reader located in the POS terminal. By means of the chip card reader, data can be read from or written to the chip card. In particular, the credit stored on the chip card is reduced by the amount payable to the merchant for the goods. A remaining credit balance remains on the chip card.

In the course of the transaction with the merchant, data is simultaneously stored in the POS terminal which contains information on the amount payable, the remaining credit balance, which financial institution operates the exchange account, and further customer data. This data is stored in the POS terminal as a transaction unit. At the end of a day, or other period of time, one or several transaction units are communicated to the financial institution operating the exchange account.The financial institution verifies whether the transaction was correctly executed by the merchant.If it is ascertained that the data in the transaction unit is based on a correct payment transaction, the payment amount is remitted to the merchant from the exchange account.

Security standards must be observed, both upon recharging of the chip card at the input terminal and upon payment by means of the chip card at the merchant's POS terminal. In order to prevent manipulations of the electronic money exchange on the chip card, security-related functions are employed for the exchange of data between the chip card and the POS terminal and for the exchange of data between the chip card and the input terminal. In particular, these functions can be handled by the encryption and decryption of data which is to be exchanged between the chip card and the respective terminal.

The precise execution of the security-related functions depends on the actual application for which the particular terminal is used. Thus, there can be provision whereby the POS terminal can be used in connection with electronic exchanges of different financial institutions. The security functions used for this purpose can be different in each case. The POS terminal must therefore be adapted to the respective exchange. In addition, an input terminal should also be usable for different electronic exchanges.

Other terminals must also be adapted to varying applications. Thus, a terminal which allows access to different applications in a network uses different procedures for different applications, which must be

executed in order to gain access to the particular application. The different procedures require different security-related functions. These must be available in each case.

Mobile security modules constitute one possibility for the flexible adaptation of terminals to different applications. Such a mobile security module is known from the specification of US Patent 4 969 188. This security module is in the form of a chip card. Stored on the chip card, in particular, are several hierarchically ordered cryptographic codes.

The known security module can be inserted into a base device. Security-related operations can then be executed in a network by means of the base device. The security-related functions required for this purpose are stored on the chip card. In this way, a separation is achieved between hardware which contains security-related data and hardware which does not contain security-related data.

A disadvantage of this well known solution is that the chip card containing the security module can only be used for a single application of the base device. If the base device is designed as a POS terminal, in connection with an electronic exchange, this means that a different chip card is required in each case for electronic exchanges of different financial institutions or even for other applications of the POS terminal.

The object of the embodiment of the present invention, therefore, is to create a mobile data carrier of the type initially referred to, which can be used flexibly for a plurality of applications.

This task is achieved, according to the embodiment of the invention, in that at least two security modules are disposed on the data carrier, with at least two security modules each comprising security-related data and/or security-related functions.

The essential advantage achieved, by comparison with prior technology, consists in the fact that it is not necessary for the mobile data carrier to be substituted in a terminal if a terminal can be used for different applications. A saving of material is achieved by the disposition of at least two security modules on the mobile data carrier. It is not necessary for a separate data carrier, with a security module in each case, to be produced for each application.

A further advantage is that, in the production of a mobile data carrier, further security modules can be disposed on the data carrier in addition to the security modules of which the intended use is already determined at the time of production. The further security modules are provided as options which can then be used if the mobile data carrier is to be used for further applications in the course of its service life.

Advantageous provision can be made whereby, by means of the at least two security modules, different applications involving a utilization of the terminal can be executed in each case. The use of one of the at least two security modules for only one particular application ensures that a user of the particular application cannot seek to acquire information about other applications.

A favorable design of the embodiment of the invention makes provision whereby, by means of the at least two security modules, it is possible to prevent execution of applications involving a utilization of the terminal. This ensures that the execution of an application can be discontinued if it is ascertained that a user is attempting to misuse the terminal.

An advantageous development makes provision whereby an operating system can be installed on the mobile data carrier, the security-related functions of the at least two security modules being executable by means of the operating system. This renders possible efficient communication between the mobile data carrier and the terminal.

Advantageous provision can be made whereby it is possible to ascertain, by means of the operating system, which of the at least two security modules can be used for an execution of a particular application involving a utilization of the terminal. By this means, any data sent from the terminal to the chip card can be assigned to the appropriate security module with a minimal expenditure of time.

The functional application of the embodiment of the invention allows the two security modules to be protected with the use of a password, by means of which it is possible to design a safeguard against improper access to the security modules.

Advantageous provision can be made whereby the at least two security modules are disposed in different areas of the memory, by means

of which, in the case of utilization of one of the two security modules, it is possible to prevent the acquisition of information from the other security module.

One of the applications which provides for the use of the terminal can, expediently, include an electronic exchange. As part of an electronic exchange, a plurality of POS terminals are to be equipped with security modules. These POS terminals are sited in different locations and are to be of use for as great a variety of exchanges as possible. The use of a mobile data carrier with at least two security modules is therefore particularly advantageous in this case.

Advantageous provision can be made whereby the security module which can be used for the application with the electronic exchange has a function for limiting an amount of money, the amount of money being the total of the credit which can be loaded on chip cards of customers of the electronic exchange. By this means, in the case of a misuse of the terminal, the resultant damage can be limited.

An advantageous design of the embodiment makes provision whereby the amount of money comprises the total of the credit in a definable period, so that it is possible to limit the period of use of the terminal for the application as part of the electronic exchange.

The limit on the amount of money can be changed, expediently, upon input of a confidential code by means of a keypad on the terminal. It can thus be ensured that the limit on the amount of money can only be changed or replaced by trustworthy persons, particularly employees of the financial institution who own the electronic exchange.

An advantageous development of the embodiment makes provision whereby the amount of money cannot be changed unless an on-line connection is formed between the terminal and a computing centre of the electronic exchange. By this means, the limit on the amount of money can be changed or replaced with relatively little expenditure and in a time-efficient manner.

A functional design of the embodiment consists in that the terminal can be designed as an off-line terminal. The limitation of the amount of money is particularly advantageous in connection with off-line terminals,

since the risk of misuse, for example in the case of stolen terminals, is particularly high with these terminals.

The advantageous applications in the dependent procedure claims disclose accordingly the advantages stated in connection with the characteristics of the device claims.

In order to promote a fuller understanding of this and other aspects of the invention, an embodiment will now be described, by way of example only, with reference to the accompanying drawing.

Fig. 1 shows a schematic representation of an arrangement for the execution of a payment transaction with a merchant. The terminal 1 includes a card reader 2. Both chip cards 3 and credit cards with magnetic strips 4 can be read by means of this card reader 2. The terminal 1 can be designed as a stand-alone device, but integration into an automatic teller machine is also conceivable. Furthermore, the terminal 1 can be connected on-line to a computing centre or even connected to a network.

In the terminal 1 there is a read/write device 5. The mobile data carrier 6 is inserted into the read/write device 5. By means of the read/write device 5, data can be exchanged between the mobile data carrier 6 and the terminal 1 and between the mobile data carrier 6 and the chip card 3 or the credit card 4.

The mobile data carrier 6 is preferably designed as a chip card. In this case, the read/write device 5 can be designed as a chip card reader. Chip cards are of a convenient format and can be mass-produced. Other possibilities for the design of the data carrier are also available to the specialist. Thus, it can be of a design similar to the structure of a plug-in card for a computer. However, if the mobile data carrier 6 is made in such a manner, it does not have the advantages stated for the chip card.

Depending on the design of the mobile data carrier 6, a read/write device 5 that is capable of communicating with the mobile data carrier 6 via an interface on the latter, is located in the terminal 1.

The mobile data carrier 6 is provided with at least two security modules 7, 8. The security modules 7, 8 are located in the memory area of

the mobile data carrier 6. They can be located in a single memory area, but it is also conceivable that the security modules 7, 8 be located in separate memory areas. Separate memory areas have the advantage that the separation hampers the acquisition of data from the security module 8 when a memory module 7 is used in the course of an use of the terminal.

Both security modules 7, 8 comprise security-related data and/or security-related functions. These security-related data include, in particular, cryptographic codes for the encryption and decryption of data which is to be exchanged.

If a customer wishes to make a payment to a merchant and use the "electronic exchange" application of his chip card 3 for this purpose, the chip card 3 is inserted into the card reader 2. The terminal 1 then sends a message to the mobile data carrier 6. This message informs the operating system installed on the mobile data carrier 6 of which application is to be executed. Using this information, the operating system selects an appropriate security module 7. This security module 7 is then available for the further execution of the application.

By means of the encryption and decryption functions of the security module 7, data can be exchanged between the chip card 3 and the terminal 1 in the course of the applications to be executed. In the case of the "electronic exchange" application, the security-related functions of the security module 7 are used, in particular, in the generation of a transaction unit and in reducing the credit balance on the chip card 3 by the amount payable to the merchant. The transaction unit comprises, for example, information relating to the customer, the merchant and the electronic exchange used.

By means of the security modules 7, 8, it is on the one hand always possible to verify, upon their use in relation to the electronic exchange, whether manipulations of the chip card 3 have occurred. Secondly, the execution of the transaction at the terminal 1 itself can be controlled by means of the security modules 7, 8. If a discrepancy is ascertained in either of the two cases, the execution of the transaction can be prevented entirely or discontinued by means of the functions in the security modules 7, 8.

If, subsequently, another customer wishes to pay with the credit card 4, the operating system of the mobile data carrier 3 selects the

security module 8 upon request by the terminal 1. The security-related functions necessary for the "credit card" application are then available.

Advantageous provision can be made whereby the security modules 7, 8 on the mobile data carrier are additionally protected by a password. The password can comprise, in particular, numbers and letters. This means that, after a security module 7, 8 has been selected for a particular application, the input of a password by the user is first required. Terminal 1 has a keypad 9 for this purpose. The security module 7, 8 only becomes available for the further execution of the application after the user has entered the correct password. If the user enters incorrect passwords repeatedly the application is discontinued.

In addition to the use of the mobile data carrier 6 with the security modules 7, 8 invention in a terminal 1, by means of which payment can be made to a merchant, it is also possible to use the mobile data carrier 6 in a bank terminal, whereby a credit can be entered on the chip card 3 at the bank terminal. In this application security-related functions are also necessary for entering the credit on to the chip card. These security-related functions are made available by means of the security modules 7, 8.

The terminal 1 can preferably also be used as an input device in connection with an electronic exchange. By means of this input device, amounts of money can be entered as credit balances, on to the chip cards 3 of the customers of the electronic exchange. The customer can then use his chip card 3 for making payments to merchants, up to the amount of this credit balance.

If the terminal 1 is also designed as an input device, the security modules 7, 8 can have a function by means of which a maximum amount can be defined for the amounts of money which can be entered. A maximum amount for a single input operation is possible, but a maximum amount for a sum of input operations is also conceivable. Once the maximum amount is reached, it is possible in one case to prevent a credit in excess of this maximum amount being entered. In another case, by means of the security modules 7, 8, it is possible to prevent further input operations being executed at the terminal 1. The maximum amount must then be replaced.

The particular maximum amount can preferably be defined at the time at which the data carrier 3 is equipped with the security module 7, 8.

However, it can also be changed in the course of the service life of the mobile data carrier. For example, authorized persons can be granted the facility of replacing or changing the maximum amount by the input of a code by means of the keypad 9. Alternatively, provision can be made whereby the maximum amount can be replaced and changed through an on-line connection of the terminal 1 to a computing centre of the owner of the electronic exchange.

The use of the maximum amount on the security modules 7, 8 in connection with off-line terminals is particularly advantageous. By this means, these terminals can be protected against unlimited misuse. If such a terminal is stolen, the loss can be limited by the fact that the input operations by means of the terminal can only be executed for a defined, limited period of time.

In summary, there has been described a mobile data carrier, particularly a chip card, with a processor, a memory and an interface, whereas the mobile data carrier is capable of insertion in a terminal, and whereas the mobile data carrier is capable of exchanging data with the terminal via the interface. At least two security modules are disposed on the mobil data carrier, whereas the at least two security modules each comprising security-related datas and/or security-related functions. With the at least two security modules applications which comprise the use of a terminal are performable.

CLAIMS

1. A mobile data carrier, particularly a chip card, with a processor, a memory and an interface, the mobile data carrier being capable of insertion in a terminal and of exchanging data with the terminal via the interface, characterized in that at least two security modules (7, 8) are disposed on the mobile data carrier (6) and that applications involving a utilization of the terminal (1) can be executed by means of at least two security modules (7, 8), the two security modules (7, 8) each comprising security-related data and/or security-related functions.

2. A mobile data carrier according to Claim 1, whereby different applications involving a utilization of the terminal (1) can be executed in each case by means of at least two security modules (7, 8).

3. A mobile data carrier according to Claim 1 or 2, whereby said security modules (7, 8) are adapted to prevent an execution of applications involving a utilization of the terminal (1).

4. A mobile data carrier according to Claim 1, 2 or 3, further comprising an operating system, whereby the security-related functions of the at least two security modules (7, 8) being executable by means of the operating system.

5. A mobile data carrier according to Claim 4, whereby said operating system is adapted to ascertain which of the at least two security modules (7, 8) can be used for an execution of a particular application involving a utilization of the terminal (1).

6. A mobile data carrier according to any of Claims 1 to 5, whereby the at least two security modules (7, 8) can each be protected by means of a password.

7. A mobile data carrier according to any of Claims 1 to 6, whereby the at least two security modules (7, 8) are located in different areas of the memory.

8. A mobile data carrier according to any one of the preceding claims, whereby one of the applications which provides for the utilization of the terminal (1) includes an electronic exchange.

9. A mobile data carrier according to Claim 8, whereby the security module which can be used for the application with the electronic exchange has a function for the limitation of an amount of money, the amount of money being the total of the credit balance which can be entered on to chip cards of customers of the electronic exchange.

10. A mobile data carrier according to Claim 9, whereby the amount of money comprises the total of the credit balance within a determined period of time.

11. A mobile data carrier according to Claim 9, whereby the limit on the amount of money can be changed upon an input of a confidential code by means of a keypad (9) of the terminal (1).

12. A mobile data carrier according to Claim 9, whereby the amount of money cannot be changed unless an on-line connection is formed between the terminal (1) and a computing centre of the electronic exchange.

13. A mobile data carrier according to Claim 9, whereby the terminal (1) can be designed as an off-line terminal.

14. A method for the exchange of data between a mobile data carrier (6), particularly a chip card, and a terminal, the mobile data carrier (6) comprising a processor, a memory and an interface, and whereby the mobile data carrier (6) be capable of insertion in the terminal; the method comprising the following steps: the installation of at least two security modules (7, 8) on the mobile data carrier (6), the at least two security modules (7, 8) each comprising security-related data and/or security-related functions, and the assignment of the at least two security modules (7, 8) to applications involving the utilization of the terminal (1).

15. A method according to Claim 14, comprising the further steps: the starting of an application involving the utilization of the terminal (1) and the selection, from the at least two security modules (7, 8), of the security module which is assigned to the application, and the exchange of application data between the terminal (1) and the selected security module.

16. A method according to Claim 15, containing the further step: the activation of the selected security module by means of a password.

17. A method according to Claim 15, containing the further step: the discontinuance of the application involving the utilization of the terminal (1) if a fault is ascertained in the execution of the application.

18. A method according to Claim 14, 15, 16 or 17 the at least two security modules (7, 8) being located in different areas of the memory of the mobile data carrier (6).

19. A mobile data carrier as substantially described herein with reference to Figure 1.

The Patent Office

13

Application No: GB 9811597.5
Claims searched: All

Examiner: Geoff Nicholls
Date of search: 21 September 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4V (VAK)

Int Cl (Ed.6): G07F 7/10

Other: ONLINE:WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	US 5578808	(TAYLOR) Whole document relevant	1, 4 to 7, 14 to 16, 18
A	US 5036461	(ELLIOTT)	
A	US 4969188	(SCHÖBI)	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.